UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/083,010 | 02/26/2002 | Matthew Charles Priestley | MS190438.1 | 4314 |

27195 7590 11/25/2008
AMIN, TUROCY & CALVIN, LLP
127 Public Square
57th Floor, Key Tower
CLEVELAND, OH 44114

| EXAMINER | |
|---|---|
| ABEDIN, SHANTO | |
| **ART UNIT** | **PAPER NUMBER** |
| 2436 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 11/25/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
lpasterchek@thepatentattorneys.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/083,010 | PRIESTLEY ET AL. | |
| | Examiner | Art Unit | |
| | SHANTO M. ABEDIN | 2436 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _03_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on _10 September 2008_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) _1,3-18,21-27,31 and 32_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1,3-15,17,18,21,23-25,27,31 and 32_ is/are rejected.

7)☒ Claim(s) _16,22 and 26_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _26 February 2002_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

## *DETAILED ACTION*

1. This office action is in response to the communication filed on 09/10/2008.

2. Claims 1, 3-18, 21-27 and 31-32 are pending in the application.

3. Claims 16, 22 and 26 are objected.

4. Claims 1, 3-15, 17-18, 21, 23-25, 27 and 31-32 have been rejected.

## ***Response to Arguments***

5. The applicant's arguments regarding the previous 35 USC 101 type rejections are fully considered, and found persuasive. The previous 35 USC 101 type rejections are withdrawn because of the amendments made to the claims.

6. The applicant's arguments regarding the previous 35 USC 112, first paragraph type rejections of claims 1 and 3-17 are fully considered, however, found not persuasive. In particular, amendments made to the claims 1 and 3-17 were unable to overcome the issues set froth by the previous 35 USC 112, second paragraph type rejections. Furthermore, upon further examination, new grounds of 35 USC 112 second paragraph type rejections are found, and presented in this office action (please see below for detail explanations).

The previous 35 USC 112, second paragraph type rejections of claims 31 and 32 are withdrawn because of the amendments made to the claims.

7. The applicant's arguments regarding the previous 35 USC 103 (a) type rejections of claims 1, 3-15, 17-18, 23-25, 27 and 31-32 are fully considered, however, found not persuasive. Regarding the previous 35 USC 103(a) type rejections, the applicant primarily argues that the cited references independently or in combination fails to disclose the limitations set forth by the amended version of

the independent claims 1, 18, 27 and 31. However, upon further consideration, the combination of the cited references was found to teach the limitations set forth by the amended claims. Therefore, the previous35 USC 103(a) type rejections of claims 1, 3-15, 17-18, 23-25, 27 and 31-32 are maintained.

## *Claim Objections*

8. Claims 1, 3-17, 27 and 31-32 are objected because of the following informalities:

***Regarding claims 1, 27 and 31,*** they are objected as claim languages being found to be unclear, or having minor grammatical error! Claims 1, 27 and 31 recite the limitations such as "a computer memory having stored thereon the following components executable by a processor ; a wrapper…., a cryptographic key..", or " a computer processor for executing the following ; means for …". However, since a semi-colon (;) is used, it is not clear what means, or components are actually included as a part of such executable components or means. The applicant is suggested to replace the semi-colon with a comma, or make appropriate correction to improve the clarity of the claim languages.

9. Claim 27 is further objected because of the following minor informalities: it recites the following limitations: it recites the limitations "a computer processor for executing the following;", and several "means for" for performing the claimed invention. However, it is unclear whether all the "means for" are referring back to a 'processor', or a processor is executing some other means!

10. ***Claim 31 is further objected*** because of the following minor informalities: it recites the following limitations:

"a wrapper generated from a pass-phrase, by the service to package the credentials, the credentials encapsulated in the wrapper, the

pass-phrase employed to mediate access to the service, the pass-phrase distributed separately from the credentials."

However, above the limitations should be written in a single paragraph to increase the clarity of the claim language!

11. ***Claim 17 is objected to under 37 CFR 1.75(c),*** as being of improper dependent form for failing to further limit the subject matter of a previous claim. In particular, claim 17 is directed to a "computer readable medium" while the independent/ parent claim 1 is directed to a 'system'! Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

12. ***Regarding claims 3-16 and 32,*** they are objected because of their dependencies on the objected claims.

Appropriate corrections are required.

## ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

13. Claims 1 and 3-17 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not

described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

***Regarding claims 1 and 3-17,*** they recite the limitations " ..the following components executable by processor; a wrapper….; and a cryptographic wrapping key..". Therefore, according to the claim limitations feature/ component such as a 'cryptographic wrapping key' is computer executable component.

However, according to the specifications, executables are different from a 'cryptographic wrapping key'. In particular, according to the specification (please see Page 12, line 21- Page 13, line 29) a wrapped credential is stored in an executable file or package or wrapper. While the storage of the cryptographic wrapping key, or a wrapper can be executable component, a cryptographic wrapping key itself can not be interpreted as an executable component (since a 'key' normally considered to be a 'string' type, not including any executable code!).

Therefore, the claim(s) contains subject matter (such as the following components executable by processor; …cryptographic wrapping key.." ) which were not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

## *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject

matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1, 6-15, 17, 27 and 31-32 are rejected under 35 USC 103 (a) as being unpatentable over Brainard ("SecureSight: An Architecture for Secure Information Access", John G Brainard, RSA Laboratories; hereinafter 'Brainard') in view of Hypponen (US 6986050 B2) further in view of Bathrick et al (US 5825300)

***Regarding claim 1,*** Brainard discloses a system that facilitates processing credentials between remote entities, comprising:

a computer memory having stored thereon ( Page 3-4; Section 2 and 2.2; credential storage in desktop or smartcard) the following components executable by a processor:

a wrapper that packages credentials associated with resources of a service (Page 2, Section 1.2 to Page 4, Section 2.2; Page 6, Section 3.5; a wrapper for secure credential communication; encrypted or locked or protected PSD, or PAC/ EAR including keys/password/ certificate also interpreted as wrapper) ; and

the cryptographic wrapping key is utilized to generate a wrapper that encapsulates the credentials ( Page 3-4 and 6, section 2.2, 2.3 and 3.5; an encryption key derived from password, or a KEK, or a PUK, or (unlocking) key is utilized to create an encrypted/ wrapped/ locked PSD or PAC that encapsulates authentication credentials/ keys/ password), and

the credentials employed to provide encrypted communication between a user and the service that facilitates access to the resources of the service (Page 2, Section 1.2 to Page 4 Section 2.2; credentials such as a key or KEK or PUK or password employed to create wrappers/ locked PSD /

encrypted PAC to provide encrypted/ secure communication in the application- based services in network; also see SSL communication).

Although Brainard further discloses the system wherein a password, or key is used to generate a cryptographic wrapping key, or protect other credentials, it fails to disclose use of a pass-phrase for that purpose, in particular, Brainard fails to disclose expressly: a cryptographic wrapping key generated from a pass-phrase; and the pass-phrase employed to facilitate access to the credentials, and the pass-phrase distributed separately from the credentials.

However, Hypponen discloses a cryptographic wrapping key generated from a pass-phrase (Col 3, lines 35-65; deriving/ generating cryptographic key from passphrase), the pass-phrase employed to facilitate access to the credentials (Col 3, lines 15-25; passphrase is employed to encrypt/decrypt password/ credential in case of password based symmetric cryptographic key).

Modified Hypponen-Brainard system fails to disclose the pass-phrase distributed separately from the credentials.

However, Bathrick et al discloses the pass phrase distributed separately from the credentials (Col 2, lines 33-40, 64-67; Claim 1; distributing keying and certificate material separately; the examiner interprets keying material as pass-phrase, and certificate material as credential).

Hypponen, Bathrick et al and Brainard are analogous art because they are from the same field of endeavor of secure electronic communication. At the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teaching of Hypponen with Brainard for generating a cryptographic wrapping key from a pass-phrase (instead of using a password) in order to provide an alternative pass-phase based protection, and to combine teachings of Bathrick et

al with modified Hypponen -Brainard system to provide further protection against unauthorized access to the passphrase and the credential.

***Regarding claim 6,*** Brainard discloses the system of claim 1, further comprising one or more partners to request access to the resources (Section 1.2, 3.3; agents, application servers/ authentication services)

***Regarding claim 7,*** Brainard discloses the system of claim 6, at least one of the partners includes a credential store to manage the credentials (Section 2.2; manager, or authentication server or application server or issuer for generating and storing credentials)

***Regarding claims 8 and 9,*** these limitations are already addressed in terms of rejecting claims 1, 6-7. Therefore, they are rejected applying as above rejecting claims 1 and 6-7.

***Regarding claims 10-12,*** Brainard discloses the system further comprising at least one of a SSL, VPN, and dedicated line (Page 6, Col 1, step 5; SSL connection); and use of that pass phrase over a SSL connection or in a VPN environment (Page 6, Col 1, step 5, application server, SSL connection); and issuing an Electronic License Certificate (Section 3.1; PAC or PSD containing certificate).

***Regarding claims 13-14,*** Brainard teaches a platform provisioning service, or such service (Page 2; Page 5, Fig 5, SecurSight authentication service; application based services on network,

and authentication services are interprettted as provisioning services ) being associated with at least one partner including at least one of a tenant and a service to form at least one of a billing, a financial, and an accounting service(Page 2; Page 5, Fig 5; system consist of manager, desktop, and application server; Brainard's enterprise network resources and applications imply capability of performing billing, financial, or accounting functions)

***Regarding claims 15 and 17,*** these limitations are already addressed in terms of rejecting claims 1, 6-7 and 13-14, therefore, they are rejected applying as above rejecting claims 1, 6-7 and 13-14.

***Regarding claim 27,*** it is rejected applying as same motivation as applied above rejecting claim 1, furthermore, Brainard discloses a system to facilitate a security relationship between parties, comprising:

a computer processor (Section 1.1, and 1.2; components; computers) for executing the following;

means for generating credentials comprising at least a password (Page 3- 6; credential generator, or issuer for generating and distributing credential/ PSD/ PAC including password);

means for generating a package of credentials by wrapping the credentials with a cryptographic wrapping key, wherein the credentials are encapsulated by the wrapper (Page 2, Section 1.2 to Page 4 Section 2.2; Page 6, Section 3.5; manager, or server, or credential issuer for generating wrapper, or encrypted PSD, PAC/ EAR; PAC or PSD containing encrypted passwords/ keys/ certificate; locking/ wrapping credential with KEK, or unlocking key)

Brainard fails to disclose means for generating a pass-phrase; and cryptographic wrapping key derived from the pass-phrase; means for transmitting the package and the pass-phrase to a system via different communications mediums; and means for storing the credentials separate from the pass-phrase.

However, Hypponen discloses means for generating a pass-phrase; and cryptographic wrapping key derived from the pass-phrase (Col 3, lines 35-65; generating cryptographic key from passphrase), the pass-phrase employed to facilitate access to the credentials (Col 3, lines 15-25; passphrase is employed to encrypt/decrypt password/ credential in case of password based symmetric cryptographic key).

Modified Hypponen-Brainard system fails to disclose means for transmitting the package and the pass-phrase to a system via different communications mediums; and means for storing the credentials separate from the pass-phrase.

However, Bathrick et al discloses means for transmitting the package and the pass-phrase to a system via different communications mediums; and means for storing the credentials separate from the pass-phrase (Col 2, lines 33-40, 64-67; Claim 1; storing, and distributing keying and certificate material separately; the examiner interprets keying material as pass-phrase, and certificate material as credential).

Furthermore, at the time of invention, it would have been obvious (from the teachings of modified Hypponen-Brainard system) to a person of ordinary skill in art to design a system wherein a pass-phrase is utilized ( instead of a password) to generate a cryptographic wrapping key, and facilitate access to the credentials.

***Regarding claim 31,*** it is rejected applying as same motivation as applied above rejecting claim 1, furthermore, Brainard discloses a system that facilitates establishing a trust relationship between entities, comprising:

a computer memory having stored thereon the following components executable by a processor (Section 1.1, and 1.2; components; computers);

a service that controls one or more resources, the service issues credentials to facilitate access to the resources (Page 2 and 5; manager, or application server for managing services on network; granting services after authenticating credentials/ PSD);

a wrapper generated by the service to package the credentials, the credentials encapsulated in the wrapper (Page 2, Section 1.2 to Page 4 Section 2.2; Page 6, Section 3.5; manager, or server, or credential issuer for generating wrapper, or encrypted PSD, PAC/ EAR; PAC or PSD containing encrypted passwords/ keys/ certificate; locking/ wrapping credential with KEK, or unlocking key)

Brainard fails to disclose expressly a wrapper generated from a pass-phrase; pass-phrase employed to generate the wrapper and mediate access to the service, the pass-phrase distributed separately from the credentials.

However, Hypponen discloses a wrapper generated from a pass-phrase (Col 3, lines 35-65; generating cryptographic key from passphrase), the pass-phrase employed to facilitate access to the credentials (Col 3, lines 15-25; passphrase is employed to encrypt/decrypt password/ credential in case of password based symmetric cryptographic key).

Modified Hypponen-Brainard system fails to disclose transmitting the package and the pass-phrase to a system via different communications mediums.

However, Bathrick et al discloses means for transmitting the package and the pass-phrase to a system via different communications mediums.

Furthermore, at the time of invention, it would have been obvious (from the teachings of modified Hypponen-Brainard system) to a person of ordinary skill in art to design a system wherein a pass-phrase is utilized ( instead of a password) to generate a cryptographic wrapping key, and facilitate access to the credentials.

***Regarding claim 32,*** Brainard discloses the system the service is a provisioning service that establishes a trust relationship between one or more partners *via* the credentials (Page 2; Page 5, Fig 5, SecurSight authentication service; application based services on network, and authentication services are interpreted as provisioning services; accessing services upon authenticating credentials or PSD).

15. Claims 3-5 are rejected under 35 USC 103 (a) as being unpatentable over Brainard ("SecureSight: An Architecture for Secure Information Access", John Brainard, RSA Laboratories; hereinafter 'Brainard') in view of Hypponen (US 6986050 B2) further in view of Bathrick et al (US 5825300) further in view of Rahman et al (US 7114080 B2)

***Regarding claim 3,*** Rahman et al discloses the credentials providing stronger encryption than the pass-phrase (Col 3, starts at line 4; Col 7, starts at line 50; using strong password; the examiner interprets such strong password usually has stronger encryption than an alphanumeric passphrase).

Rahman et al and Brainard are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Rahman et al with modified Brainard method to design a method wherein credentials providing stronger encryption than the pass-phrase in order to provide transferring of a strong credential.

***Regarding claim 4,*** Rahman et al discloses the credentials providing greater than 100 bits ofencryption (Col 3, starts at line 4; Col 7, starts at line 50; using strong password).

***Regarding claim 5,*** Hypponen discloses the pass-phase having human-readable alpha-numeric characteristics. (Col 1, lines 40-65; passphrases)

16. Claim 18, 21 and 23-25 are rejected under 35 USC 103 (a) as being unpatentable over Hypponen (US 6986050 B2) in view of Brainard (SecurSight: An Architecture for Secure Information Access, RSA Laboratories) further in view of Bathrick et al (US 5825300).

***Regarding claim 18,*** Hypponen discloses a method to facilitate a security connection between entities, comprising:

generating a strong password via a random generation function associated with a standard platform ( Col 2, line 51 – Col 3,, line 30; generating long passwords);

generating a human readable pass-phrase (Col 2, line 51 – Col 3,, line 30; generating human readable long passphrase or password);

deriving a wrapping key from the pass-phrase (Col 3, lines 35-65; generating cryptographic key from passphrase);

wrapping the password cryptographically *via* the pass-phrase (Col 5, starts at line 1; encrypting password with passphrase);

storing the wrapped password (Col 5, starts at line 1; storing encrypted password) ; and

transmitting the executable and the pass-phrase to a remote user system separately *via* different

communications mediums, wherein the remote user employs the pass-phrase to unlock the strong password stored, the strong password employed to establish a trust relationship with an entity (Col 5, starts at line 1).

Hypponen fails to disclose expressly wherein the wrapping key facilitates in encapsulating the password in a wrapper; storing the wrapped password in an executable; and transmitting the executable and the pass-phrase to a system separately via different communications mediums.

However, Brainard discloses wherein the wrapping key facilitates in encapsulating the password in a wrapper (Page 4 and 6, section 2.2, 2.3 and 3.5; an encrypted/ wrapped/ locked PSD or PAC that encapsulates authentication credentials such as keys or password; using a cryptographic key to wrap or lock the credentials/ PSD/ PAC); and storing the wrapped password in an executable (Pages 3-5; storage of PSD and PAC as executable codes, and cookies);

Modified Brainard - Hypponen system fails to disclose expressly transmitting the executable and the pass-phrase to a system via different communications mediums. However, Bathrick et al discloses transmitting the executable and the pass-phrase to a system via different

communications mediums (Col 2, lines 33-40, 64-67; Claim 1; distributing keying material, and certificate material separately).

Brainard, Bathrick et al and Hypponen are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teaching of Bathrick et al with modified Brainard - Hypponen system to provide further protection against unauthorized access to the passphrase and the credential.

***Regarding claim 21,*** Brainard teaches a method comprising at least one of: requesting a SSL connetion; and presenting an SSL certificate in response to the request (Section 3.3" Use of PACs by connect agent; Section 4.2: Certificate Validation Service; Brainard teaches an application access agent and a certificate validation service to validate SSL certificates)

***Regarding claim 23,*** Brainard teaches limiting access to the executable (Section 2.2, 2.3, 4.2; accessing the wrapped credentials, PAC upon authentication)

***Regarding claim 24,*** Brainard teaches the method comprising at least one of: setting up account privileges; designating account contacts; and verifying contacts (Page 7, Col 1, Table 2, EAR; access right).

***Regarding claim 25,*** Bathrick et al discloses a method comprising verbally communicating the password (Claim 3; non electronic communication medium for keying material/password).

## ***Allowable Subject Matter***

17. Claims 16, 22 and 26 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

## ***Conclusion***

**18. Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner. Finally, for any future amendments to claims, the applicant is respectfully suggested to incorporate the paragraph numbers from the specification upon which the support for such amendments were obtained.

**19. THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:30 AM to 7:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is

assigned is 703-872-9306. The RightFax number for faxing directly to the examiner is 571-273-3551.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436